

Feuille d'exercices n° 3 : Groupe des permutations

Exercice 1 Exprimer comme produit de cycles disjoints :

1. $(1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$;
2. $(1\ 2)(1\ 2\ 3)(1\ 2)$.

Quelle est la signature de ces permutations ?

Solution 1

1. Posons $\sigma_1 = (1\ 2\ 3)(4\ 5)(1\ 6\ 7\ 8\ 9)(1\ 5)$. Explicitons σ_1 :

1	2	3	4	5	6	7	8	9
5	2	3	4	1	6	7	8	9
5	2	3	4	6	7	8	9	1
4	2	3	5	6	7	8	9	1
4	3	1	5	6	7	8	9	2

Donc $\sigma_1 = (4\ 3\ 1\ 5\ 6\ 7\ 8\ 9\ 2)$.

C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

2. Posons $\sigma_2 = (1\ 2)(1\ 2\ 3)(1\ 2)$. Explicitons σ_2 :

1	2	3
2	1	3
3	2	1
3	1	2

Ainsi $\sigma_2 = (3\ 1\ 2)$.

C'est une permutation paire, de signature 1 ; en effet la signature d'un cycle d'ordre p est $(-1)^{p-1}$.

Exercice 2 Calculer aba^{-1} pour

1. $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$;
2. $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$.

Solution 2

1. Calcul de aba^{-1} pour $a = (1\ 3\ 5)(1\ 2)$, $b = (1\ 5\ 7\ 9)$.

Explicitons a :

1	2	3	4	5	6	7	8	9
2	1	3	4	5	6	7	8	9
2	3	5	4	1	6	7	8	9

autrement dit $a = (1\ 2\ 3\ 5)$. Il s'en suit que

1	2	3	4	5	6	7	8	9
5	1	2	4	3	6	7	8	9

Finalement nous obtenons

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 2 & 4 & 3 & 6 & 7 & 8 & 9 \\ 7 & 5 & 2 & 4 & 3 & 6 & 9 & 8 & 1 \\ 7 & 1 & 3 & 4 & 5 & 6 & 9 & 8 & 2 \end{array}$$

2. Calcul de aba^{-1} pour $a = (5\ 7\ 9)$, $b = (1\ 2\ 3)$. Les cycles a et b sont à supports disjoints donc commutent. Ainsi $aba^{-1} = aa^{-1}b = b$, autrement dit $aba^{-1} = b$.

Exercice 3 Déterminer la parité des permutations suivantes et les écrire comme produits de transpositions :

$$\sigma_1 = (1\ 3\ 5)(5\ 4\ 3\ 2)(5\ 6\ 7\ 8), \quad \sigma_2 = (1\ 2)(2\ 4)(1\ 7)(7\ 6\ 8).$$

Solution 3 L'application signature est un morphisme de $\mathcal{S}_8$ dans le groupe multiplicatif $\{-1, 1\}$.

La permutation σ_1 est le produit d'un cycle pair avec deux cycles impairs, elle est donc paire.

La permutation σ_2 est le produit de 3 cycles impairs et d'un cycle pair, elle est donc impaire.

Autre méthode :

$$\sigma_1 = (3\ 5)(5\ 1)(2\ 3)(4\ 2)(2\ 5)(7\ 8)(6\ 8)(5\ 8)$$

donc $\text{sgn}(\sigma_1) = (-1)^8 = 1$ et

$$\sigma_2 = (1\ 2)(2\ 4)(1\ 7)(6\ 8)(7\ 8)$$

donc $\text{sgn}(\sigma_2) = (-1)^5 = -1$.

Exercice 4 Soit σ la permutation de $\{1, 2, \dots, 12\}$ définie par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$$

Calculer σ^{2000} .

Solution 4 Posons $\sigma_1 = (1\ 10\ 5\ 7\ 2\ 9\ 12)$, $\sigma_2 = (3\ 8\ 6)$ et $\sigma_3 = (4\ 11)$.

Ces trois permutations sont à supports disjoints deux à deux donc commutent. Il en résulte que $\sigma^{2000} = \sigma_1^{2000}\sigma_2^{2000}\sigma_3^{2000}$.

Par ailleurs σ_1 est d'ordre 7 et $2000 = 285 \times 7 + 5$ d'où $\sigma_1^{2000} = \sigma_1^5$.

De plus σ_2 est d'ordre 3 et $2000 = 666 \times 3 + 2$ d'où $\sigma_2^{2000} = \sigma_2^2$.

Enfin σ_3 est d'ordre 2 et $2000 = 1000 \times 2$ d'où $\sigma_3^{2000} = \text{id}$.

Par suite

$$\sigma^{2000} = \sigma_1^5 \sigma_2^2 = (1\ 9\ 7\ 10\ 12\ 2\ 5)(3\ 8\ 6)$$

Exercice 5 Soit n un entier, soit σ une permutation de $\{1, 2, \dots, n\}$ et soit $(x_1\ x_2\ \dots\ x_k)$ un cycle de $\mathcal{S}_n$.

Calculer $\sigma(x_1\ x_2\ \dots\ x_k)\sigma^{-1}$.

Solution 5 Pour $1 \leq i \leq k$ posons $\sigma(x_i) = y_i$. Alors $\sigma^{-1}(y_i) = x_i$ et $((x_1\ x_2\ \dots\ x_k)\sigma^{-1})(y_i) = ((x_1\ x_2\ \dots\ x_k))(x_i) = x_{i+1}$ donc $\sigma(x_1\ x_2\ \dots\ x_k)\sigma^{-1}(y_i) = \sigma(x_{i+1}) = y_{i+1}$.

Par ailleurs si $y \notin \{y_1, y_2, \dots, y_k\}$, alors $(\sigma(x_1\ x_2\ \dots\ x_k)\sigma^{-1})(y) = y$.

Il en résulte que

$$\sigma(x_1\ x_2\ \dots\ x_k)\sigma^{-1} = (\sigma(x_1)\ \sigma(x_2)\ \dots\ \sigma(x_k))$$

Exercice 6 Dans le groupe $\mathcal{S}_7$ calculer le produit

$$(4\ 5\ 6)(5\ 6\ 7)(6\ 7\ 1)(1\ 2\ 3)(2\ 3\ 4)(3\ 4\ 5).$$

Solution 6 Nous avons

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 5 & 3 & 6 & 7 \\ 1 & 3 & 2 & 5 & 4 & 6 & 7 \\ 2 & 1 & 3 & 5 & 4 & 6 & 7 \\ 2 & 6 & 3 & 5 & 4 & 7 & 1 \\ 2 & 7 & 3 & 6 & 4 & 5 & 1 \\ 2 & 7 & 3 & 4 & 5 & 6 & 1 \end{array}$$

Exercice 7 Soit n un entier. Construire des homomorphismes injectifs de $\mathcal{S}_n$ dans $\mathcal{S}_{n+1}$.

Solution 7 Soit x un élément de $\{1, 2, \dots, n+1\}$. Posons $E_x = \{1, 2, \dots, n+1\} \setminus \{x\}$. Il existe un isomorphisme φ entre $\mathcal{S}_n$ et $\mathcal{S}_{E_x}$. Le morphisme $f_x: \mathcal{S}_n \rightarrow \mathcal{S}_{n+1}$ défini par

$$\begin{cases} f_x(\sigma)(i) = \varphi(\sigma)(i) \text{ pour } i \in E_x \\ f_x(\sigma)(x) = x \end{cases}$$

est injectif.

Exercice 8 Montrer que si c et γ sont des n -cycles de $\mathcal{S}_n$ qui commutent entre eux, il existe un entier r tel que $\gamma = c^r$.

Solution 8 Soient $c = (1 \ c(1) \ c^2(1) \ \dots \ c^{n-1}(1))$ et $\gamma = (1 \ \gamma(1) \ \gamma^2(1) \ \dots \ \gamma^{n-1}(1))$ deux n -cycles de $\mathcal{S}_n$ qui commutent entre eux, *i.e.* $c\gamma = \gamma c$.

L'ensemble $\{1, 2, \dots, n\}$ coïncide avec $\{1, c(1), c^2(1), \dots, c^{n-1}(1)\}$. Par conséquent il existe $0 \leq r \leq n-1$ tel que $\gamma(1) = c^r(1)$. De plus si $i \in \{1, \dots, n\}$, alors il existe $0 \leq s \leq n-1$ tel que $i = c^s(1)$. Il en résulte que

$$\gamma(i) = \gamma(c^s(1)) = c^s(\gamma(1)) = c^s(c^r(1)) = c^r(c^s(1)) = c^s(i).$$

Par suite $\gamma = c^s$.

Autre méthode : faisons agir $\mathcal{S}_n$ sur l'ensemble des n -cycles par conjugaison (c'est possible car les n -cycles sont dans la même orbite pour cette action). Cet ensemble est de cardinal $(n-1)!$ En effet un n -cycle σ s'écrit $(1 \ \sigma(1) \ \sigma(2) \ \dots \ \sigma(n-1))$ et nous avons $(n-1)$ choix pour $\sigma(1)$ puis $(n-2)$ choix pour $\sigma(2)$ etc. Le groupe $\mathcal{S}_n$ agit transitivement sur cet ensemble. L'indice du stabilisateur de c pour cette action est $(n-1)!$ et son cardinal est n . Ce stabilisateur est le centralisateur de c qui contient au moins les n puissances de c et tout n -cycle qui commute avec c est donc égal à une puissance de c .

Exercice 9 Soit $n \geq 3$ un entier. Sachant que le groupe $\mathcal{S}_n$ est engendré par l'ensemble des transpositions de $\{1, 2, \dots, n\}$ montrer que $\mathcal{S}_n$ est engendré par les ensembles suivants de permutations :

1. $(1 \ 2), \dots, (1 \ n)$;
2. $(1 \ 2), (2 \ 3), \dots, (n-1 \ n)$;
3. $(1 \ 2), (2 \ 3 \ \dots \ n)$.

Solution 9

1. Notons que $(i \ j) = (i \ 1)(j \ 1)(i \ 1)$ lorsque $i \neq j$;
2. Soit $i < j$.
Si $j > i+1$, alors

$$(i \ j) = (j-1 \ j)(i \ j-1)(j-1 \ j) \tag{1}$$

Si $j-1 = i+1$, alors $(i \ j) \in \langle (1 \ 2), (2 \ 3), \dots, (n-1 \ n) \rangle$.

Sinon nous appliquons (1) en remplaçant $(i \ j)$ par $(i \ j-1)$ et nous arrivons de proche en proche au résultat.

3. Nous avons

$$(2 \ 3 \ \dots \ n)(1 \ 2)(2 \ 3 \ \dots \ n)^{-1} = (1 \ 3).$$

Par suite par récurrence pour $i > 2$ nous avons

$$(1 \ i) = (2 \ 3 \ \dots \ n)^{i-2}(1 \ 2)(2 \ 3 \ \dots \ n)^{-i+2}$$

d'où le résultat (en utilisant la première question).

Exercice 10 Soit G un sous-groupe de $\mathcal{S}_4$ opérant sur $\{1, 2, 3, 4\}$ par l'action induite par l'action naturelle de $\mathcal{S}_4$.

Pour $i = 1, 2, 3, 4$ on note $\mathcal{O}_i$ l'orbite de i et S_i le stabilisateur de i .

Déterminer $\mathcal{O}_i$ et S_i pour $i = 1, 2, 3, 4$ dans chacun des cas suivants :

1. $G = \langle (1 \ 2 \ 3) \rangle$;
2. $G = \langle (1 \ 2 \ 3 \ 4) \rangle$;
3. $G = \{e, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$;
4. $G = \{e, (1 \ 2), (1 \ 2)(3 \ 4), (3 \ 4)\}$;
5. $G = \mathcal{A}_4$.

Solution 10

1. Supposons que $G = \langle (1 \ 2 \ 3) \rangle$.
 Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \text{id}$.
 Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \text{id}$.
 Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3\}$ et $S_i = \text{id}$.
 Si $i = 4$, alors $\mathcal{O}_i = \{4\}$ et $S_i = G$.
2. Supposons que $G = \langle (1 \ 2 \ 3 \ 4) \rangle$.
 Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
 Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
 Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
 Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
3. Supposons que $G = \{\text{id}, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\}$.
 Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
 Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
 Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
 Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \text{id}$.
4. Supposons que $G = \{\text{id}, (1 \ 2), (1 \ 2)(3 \ 4), (3 \ 4)\}$.
 Si $i = 1$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\text{id}, (3 \ 4)\}$.
 Si $i = 2$, alors $\mathcal{O}_i = \{1, 2\}$ et $S_i = \{\text{id}, (3 \ 4)\}$.
 Si $i = 3$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\text{id}, (1 \ 2)\}$.
 Si $i = 4$, alors $\mathcal{O}_i = \{3, 4\}$ et $S_i = \{\text{id}, (1 \ 2)\}$.
5. Supposons que $G = \mathcal{A}_4$.
 Si $i = 1$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (2 \ 3 \ 4) \rangle$.
 Si $i = 2$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (1 \ 3 \ 4) \rangle$.
 Si $i = 3$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (1 \ 2 \ 4) \rangle$.
 Si $i = 4$, alors $\mathcal{O}_i = \{1, 2, 3, 4\}$ et $S_i = \langle (1 \ 2 \ 3) \rangle$.

Exercice 11 Établir la table de $\mathcal{S}_3$ et de $\mathbb{Z}/6\mathbb{Z}$.

Quels sont les sous-groupes de $\mathcal{S}_3$?

Quels sont les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$?

Solution 11 La table de $\mathcal{S}_3$ est

	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(1 2 3)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

La table de $\mathbb{Z}/6\mathbb{Z}$ est

	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[4]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

Les sous-groupes de $\mathcal{S}_3$ sont :

- un sous-groupe d'ordre 1 ;
- trois sous-groupes d'ordre 2 : $\langle (1\ 2) \rangle$, $\langle (1\ 3) \rangle$, $\langle (2\ 3) \rangle$;
- un sous-groupe d'ordre 3 : $\langle (1\ 2\ 3) \rangle$.

Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont :

- un sous-groupe d'ordre 1 ;
- un sous-groupes d'ordre 2 : $\langle [3] \rangle$;
- un sous-groupes d'ordre 3 : $\langle [2] \rangle$.

Exercice 12

- Déterminer les classes de conjugaison dans $\mathcal{S}_n$.
- Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Solution 12

- Soit $c = (a_1 \dots a_k)$ un k -cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n . Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \dots \leq m_r \qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i .

- Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau \sigma \tau^{-1} = (\tau c) \sigma (\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \dots a_{2k+1}) \qquad c' = (a'_1 \dots a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \dots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

$$\tau \sigma \tau^{-1} = (\tau d) \sigma (\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ . On voit que $(i\ j)\sigma(i\ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 13 Considérons les deux éléments suivants du groupe symétrique $\mathcal{S}_9$

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$$

$$\sigma_2 = (1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in \mathcal{S}_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$.

Quel est le cardinal (une expression sous forme de produit d'entiers suffit) de la classe de conjugaison de σ_1 dans $\mathcal{S}_9$?

Solution 13 Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de même longueur (2, 3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9)$$

$$\sigma_2 = (8\ 9)(5\ 6\ 7)(1\ 2\ 3\ 4)$$

nous trouvons parmi de nombreux choix possibles $\omega = (1\ 8\ 3\ 5\ 7\ 2\ 9\ 4\ 6)$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de $\mathcal{S}_9$ de type 2, 3, 4 :

- $(9 \cdot 8)/2 = 9 \cdot 4$ choix possibles pour la transposition ;
- $2 \cdot (7 \cdot 6 \cdot 5)/6 = 7 \cdot 5 \cdot 2$ choix possibles pour le 3-cycle ;
- 6 choix possibles pour le 4-cycle.

soit finalement $9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$ choix possibles.

Exercice 14 Montrer que le groupe symétrique $\mathcal{S}_3$ est isomorphe à son groupe d'automorphisme $\text{Aut}(\mathcal{S}_3)$.

Solution 14 L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathcal{S}_3$ dans $\text{Aut}(\mathcal{S}_3)$, car le centre de $\mathcal{S}_3$ est trivial.

De plus un élément de $\text{Aut}(\mathcal{S}_3)$ est déterminé par l'image des générateurs (12) et (13). Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathcal{S}_3$), donc en comparant les ordres nous obtenons que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 15 Montrer que tout sous-groupe d'indice n dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

Solution 15 Soit H un sous-groupe d'indice n dans $\mathcal{S}_n$.

Si $n \geq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors si $H \not\cong \mathcal{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q - 1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathcal{S}_n$, et donc aussi H , opère par translation à gauche sur $E = \mathcal{S}_n/H$ d'où un homomorphisme

$$\varphi: \mathcal{S}_n \rightarrow \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker \varphi = \bigcap_{a \in \mathcal{S}_n} aHa^{-1}$, $\ker \varphi$ est distingué dans $\mathcal{S}_n$ et $\ker \varphi \subset H$ on a $\ker \varphi = \{\text{id}\}$ (rappel : pour $n \geq 5$

les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\text{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de $\text{id}H$ on a : $\varphi(H) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$.

Exercice 16

- a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.
- b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Solution 16

- a) Soit $c = (a_1 \dots a_k)$ un k -cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n . Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \dots \leq m_r \qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i .

- b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau \sigma \tau^{-1} = (\tau c) \sigma (\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \dots a_{2k+1}) \qquad c' = (a'_1 \dots a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \dots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

$$\tau \sigma \tau^{-1} = (\tau d) \sigma (\tau d)^{-1}$$

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ . On voit que $(i \ j) \sigma (i \ j)$ n'est pas conjugué à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 17 Soit n un entier. Rappelons que $\mathcal{A}_n$ est le sous-groupe de $\mathcal{S}_n$ formé par les permutations paires.

- a) Montrer que le produit de deux transpositions distinctes de $\mathcal{S}_n$ est un 3-cycle ou un produit de deux 3-cycles. En déduire que $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles de $\mathcal{S}_n$.
- b) i) Montrer que pour $n \geq 3$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des 3-cycles $(1 \ 2 \ 3), \dots, (1 \ 2 \ n)$.
En déduire que $\mathcal{A}_n$ est pour $n \geq 3$ stable par tout automorphisme ϕ de $\mathcal{S}_n$ (autrement dit $\mathcal{A}_n$ est un sous-groupe caractéristique de $\mathcal{S}_n$).
- ii) Montrer que $\mathcal{A}_n$ est engendré
— si n est impair ≥ 5 par $(1 \ 2 \ 3)$ et $(3 \ 4 \dots n)$;
— si n est pair ≥ 4 par $(1 \ 2 \ 3)$ et $(1 \ 2)(3 \ 4 \dots n)$.
- c) Montrer que pour $n \geq 5$ le groupe $\mathcal{A}_n$ est engendré par l'ensemble des permutations de $\mathcal{S}_n$ de la forme $(a \ b)(c \ d)$ avec a, b, c, d deux à deux distincts.

Solution 17

- a) Soient $i < j < k < l$. Nous avons

$$(i \ j)(k \ l) = (i \ j)(j \ k)(j \ k)(k \ l)$$

Or $(i \ j)(j \ k) = (i \ j \ k)$ donc

$$(i \ j)(k \ l) = (i \ j \ k)(j \ k \ l).$$

Tout élément σ de $\mathcal{A}_n$ est le produit d'un nombre pair de transpositions donc un produit de 3-cycles. Le sous-groupe de $\mathcal{A}_n$ engendré par les 3-cycles contient donc $\mathcal{A}_n$, c'est donc $\mathcal{A}_n$.

- b) i) Soient i, j et k des éléments de $\{1, \dots, n\}$ tels que $i < j < k$. Nous avons

$$(i \ j \ k) = (1 \ 2 \ i)(2 \ j \ k)(1 \ 2 \ i)^{-1}$$

et

$$(2 \ j \ k) = (1 \ 2 \ j)(1 \ 2 \ k)(1 \ 2 \ j)^{-1}$$

donc $\mathcal{A}_n \subset \langle (1 \ 2 \ 3), \dots, (1 \ 2 \ n) \rangle$. Il en résulte que

$$\mathcal{A}_n = \langle (1 \ 2 \ 3), \dots, (1 \ 2 \ n) \rangle.$$

Soient ϕ un automorphisme de $\mathcal{S}_n$ et σ un 3-cycle. L'ordre de $\phi(\sigma)$ est 3. Donc $\phi(\sigma)$ est un produit de 3-cycles car son ordre est le ppcm des longueurs des cycles qui interviennent dans sa décomposition en cycles. Le groupe $\mathcal{A}_n$ est donc caractéristique dans $\mathcal{S}_n$.

ii) Pour $i \geq 4$ et $n \geq 4$ nous avons

$$(1 \ 2 \ i) = (3 \ 4 \ \dots \ n)^{i-3}(1 \ 2 \ 3)(3 \ 4 \ \dots \ n)^{-3+i}.$$

Par ailleurs si $n \geq 5$ est impair, $(3 \ 4 \ \dots \ n)$ est une permutation paire car c'est un cycle de longueur impaire $n - 2$. Ainsi pour $n \geq 5$ impair on a

$$\mathcal{A}_n = \langle (1 \ 2 \ 3), (3 \ 4 \ \dots \ n) \rangle$$

Nous avons

$$(1 \ 2)^\alpha (1 \ 2 \ i) (1 \ 2)^\alpha = \begin{cases} (1 \ 2 \ i) & \text{pour } \alpha \text{ pair} \\ (1 \ 2 \ i)^{-1} & \text{pour } \alpha \text{ impair} \end{cases}$$

Donc puisque pour $i \geq 4$ et $n \geq 4$

$$(1 \ 2 \ i) = (3 \ 4 \ \dots \ n)^{i-3}(1 \ 2 \ 3)(3 \ 4 \ \dots \ n)^{-3+i}.$$

alors pour $i \geq 4$ impair et $n \geq 4$

$$(1 \ 2 \ i) = [(1 \ 2)(3 \ 4 \ \dots \ n)]^{i-3}(1 \ 2 \ 3)[(1 \ 2)(3 \ 4 \ \dots \ n)]^{-3+i}.$$

Et pour $i \geq 4$ pair et $n \geq 4$

$$(1 \ 2 \ i) = [((1 \ 2)(3 \ 4 \ \dots \ n))^{i-3}(1 \ 2 \ 3)((1 \ 2)(3 \ 4 \ \dots \ n))^{-3+i}]^{-1}.$$

Or si $n \geq 4$ est pair $(1 \ 2)(3 \ 4 \ \dots \ n)$ est une permutation paire. Par conséquent le groupe $\mathcal{A}_n$ est engendré par $(1 \ 2 \ 3)$ et $(1 \ 2)(3 \ 4 \ \dots \ n)$.

c) Il suffit de montrer que tout 3-cycle $(i \ j \ k)$ (avec $i < j < k$) est produit de permutations de la forme $(a \ b)(c \ d)$ où a, b, c et d sont deux à deux distincts. Puisque $n \geq 5$ il existe ℓ et m dans $\{1, 2, \dots, n\}$ tels que i, j, k, ℓ et m soient 2 à 2 distincts. Or nous avons

$$(i \ j \ k) = (m \ \ell)(j \ k)(m \ \ell)(i \ k)$$

d'où le résultat.